Socket

Care must be exercised when a process with elevated permissions grants or allows children processes to inherit its rights.

Sean Barnum, Cigital, Inc. [vita[1]]

2007-04-17

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 2575 bytes

<table>
<tr><td>Attack Category</td><td>• Denial of Service</td></tr>
<tr><td>Vulnerability Category</td><td>• Privilege escalation problem</td></tr>
<tr><td>Software Context</td><td>• Inheritance
• Networking</td></tr>
<tr><td>Location</td><td>• sys/socket.h</td></tr>
<tr><td>Description</td><td>Care must be exercised when a process with elevated permissions grants or allows children processes to inherit its rights.

The socket function creates an endpoint for communication and returns a descriptor to the calling process.

An inherited socket with broad permissions (e.g., root) could enable the establishment of a privileged connection to another machine making it vulnerable to further attack.</td></tr>
<tr><td>APIs</td><td><table><tr><th>Function Name</th><th>Comments</th></tr><tr><td>socket()</td><td></td></tr></table></td></tr>
<tr><td>Method of Attack</td><td>An attacker can cause a denial-of-service using ioctl functions with the children of a process that have inherited a socket from a root process.</td></tr>
<tr><td>Exception Criteria</td><td></td></tr>
<tr><td>Solutions</td><td><table><tr><th>Solution Applicability</th><th>Solution Description</th><th>Solution Efficacy</th></tr><tr><td>Always</td><td>Avoid giving un-trusted child processes sockets with root privileges.</td><td>Effective if malicous child processes are not given sockets with root access.</td></tr></table></td></tr>
<tr><td>Signature Details</td><td></td></tr>
<tr><td>Examples of Incorrect Code</td><td></td></tr>
</table>

1. http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

Examples of Corrected Code	
Source References	• http://unixhelp.ed.ac.uk/CGI/man-cgi?socket+2 • ITS4 Source Code Vulnerability Scanning Tool [3]
Recommended Resource	
Discriminant Set	**Operating System** **Language**

Cigital, Inc. Copyright

1. mailto:copyright@cigital.com